The devil is in ~~details~~ asymmetries

Edinah K. Gnang and Vidit Nanda

Abstract. We formally investigate some computational obstacles to tractability of computing the variety determined by K complex polynomials in N boolean variables. We show that using algebraic methods for solving combinatorial problems, the obstacles to tractability lies in the order of magnitude of asymmetries admitted by the given system of equations.

1. Introduction

Let N and K be natural numbers which remain fixed throughout the paper. Recall that $\mathbb{C}[x_1,\ldots,x_N]$ denotes the ring of complex polynomials in the N variables $x_1,\ldots,x_N$, and let $\mathcal{I}$ be the ideal generated by $\left\{x_n^2 - x_n\right\}_1^N$. Let $\mathcal{C} = {}^{\mathbb{C}[x_1,\ldots,x_n]}/_{\mathcal{I}}$ be the ring of complex polynomials in N Boolean variables. We investigate the tractability of computing the variety $Z(\mathcal{F})$ corresponding to the simultaneous zeros of K given polynomials $\mathcal{F} = \{f_k\}_1^K \subset \mathcal{C}$, each of which have at most n terms. Recall that $\mathbb{C}[x_1,\ldots,x_N]$ – and hence, $\mathcal{C}$ – admits a natural action of the symmetric group Σ_N obtained by permuting the variables $\{x_n\}_1^N$. More precisely, for each $\sigma \in \Sigma_N$ and $f \in \mathbb{C}[x_1,\ldots,x_N]$ we define $\sigma \circ f \in \mathcal{C}$ by

$$\sigma \circ f(x_1,\ldots,x_n) = f(x_{\sigma(1)},\ldots,x_{\sigma(N)}).$$

Recall the polynomials fixed by this action of Σ_N are called the *symmetric polynomials* of $\mathbb{C}[x_1,\ldots,x_N]$.

For each $\sigma \in \Sigma_N$, define the *σ-permuted system* $\mathcal{F}_\sigma \subset \mathcal{C}$ by $\mathcal{F}_\sigma = \{\sigma \circ f_k\}_1^N$. The *stabilizer* of the system $\mathcal{F}$ is the subgroup of Σ_N defined as follows

$$\mathrm{Stab}(\mathcal{F}) = \{\sigma \in \Sigma_N \mid \mathcal{F}_\sigma = \mathcal{F}\}$$

2. The Polynomial method for solving Combinatorial problems with bounded size destabilizers

Theorem 2.1. *If $|\Sigma_N \smallsetminus \mathrm{Stab}(\mathcal{F})| = c \leq c_0$ for some constant c_0 then the problem of determining $Z(\mathcal{F})$ is in co-NP.*

Proof. We wish to determine whether the following algebraic variety is non-empty.

$$Z(\mathcal{F}) = \left\{(x_1,\ldots,x_N) \in \{0,1\}^N \mid f_k(x_1,\ldots,x_N) = 0 \text{ for each } 1 \leq k \leq K\right\}$$

Consider the following iteration

$$\begin{aligned} f_{k,\{\sigma_1,\sigma_2\}} &= (\sigma_1 \circ f_k) \cdot (\sigma_2 \circ f_k) \mod \mathcal{I} \\ &\vdots \\ f_{k,\{\sigma_0,\cdots,\sigma_{c-1}\}} &= f_{k,\{\sigma_0,\cdots,\sigma_{c-2}\}} \cdot (\sigma_{c-1} \circ f_k) \mod \mathcal{I} \end{aligned} \tag{2.1}$$

where

$$\Sigma_N \smallsetminus \mathrm{Stab}(\mathcal{F}) := \{\sigma_0,\cdots,\sigma_{c-1}\}.$$

So as to induce the following set of polynomials each having at most n^c terms, all square free.

$$\mathcal{G} := \left\{f_{k,\{\sigma_0,\cdots,\sigma_{c-1}\}}\right\}_{0\leq k<N}. \tag{2.2}$$

We can determine a polynomial $p\left(x_0\right)$ in a single variable

$$p\left(x_0\right)=\prod_{0\leq t<N}\left(x_0-\beta_t\right) \tag{2.3}$$

in the ideal generated by the polynomials in $\mathcal{G}$ i.e. $\exists\ \left\{h_k\right\}_{0\leq k<n}\subset\mathcal{C}$ such that

$$p\left(x_0\right)=\sum_{0\leq k<K}h_k\cdot f_{k,\{\sigma_0,\cdots,\sigma_{c-1}\}}. \tag{2.4}$$

Henceforth, let $\boldsymbol{\beta}$ denote the vector whose entries are the roots of the polynomial $p\left(x_0\right)$. If $\boldsymbol{\beta}$ admits an index t for which $\beta_t\notin\mathbb{F}_2$ than this fact constitutes a certificate of non existence of solution to $\mathcal{F}$. However it would be incorrect to conclude that if $\forall\ 0\leq t<N$, $\beta_t\in\mathbb{F}_2$ there should necessarily exist solutions to $\mathcal{F}$. The criteria invoked above is therfore a necessary but not a sufficient condition for the existence of solution to $\mathcal{F}$. The sufficient condition for the existence of solution to $\mathcal{F}$ is the fact that the matrix $\mathbf{M}_{\mathcal{F}}$ of size $N\times c$, whose entries are given by

$$\mathbf{M}_{\mathcal{F}}:=\left(m_{k,\sigma}=\sigma\circ f_k\right) \tag{2.5}$$

(where $0\leq k<K$ and $\sigma\in\Sigma_N\setminus\mathrm{Stab}(\mathcal{F})$), has the property that $\mathbf{M}_{\mathcal{F}}\mod\left(\mathbf{x}-\boldsymbol{\beta}\right)$, has at least one zero column. □

References

[1] Russell Impagliazzo, Pavel Pudlk, Jiri Sgall: Lower Bounds for the Polynomial Calculus and the Groebner Basis Algorithm Electronic Colloquium on Computational Complexity (ECCC) 4(42): (1997)

[2] Matthew Clegg, Jeff Edmonds, Russell Impagliazzo: Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability. STOC 1996: 174-183

[3] @ArticleABRW01, author=Mikhail Alekhnovich and Eli Ben-Sasson and Alexander Razborov and Avi Wigderson, title=Space Complexity in Propositional Calculus, journal=SIAM Journal of Computing, volume=31, number=4, pages=1184-1211, year=2001,